BRADFORD NETWORKS AND FORTINET

SOLUTION OVERVIEW

Networks are undergoing dramatic change with BYOD, IoT and private, public, and hybrid clouds in addition to a highly-mobile workforce and geographically-dispersed data centers. Securing highly dynamic and distributed environments requires integrated security and network technologies that share intelligence and collaborate to detect and respond to threats. The Fortinet and Bradford Networks partnership combines the SIEM, switch, secure WiFi or firewall benefits of Fortinet, with the visibility, network access control and automated threat response of Network Sentry. By combining these technologies, organizations achieve superior threat detection for mobile, IoT and network devices.

Network Sentry provides visibility and control of all wired and wireless infrastructures to extend the Fortinet Security Fabric to all equipment. By combining Fortinet solutions with Network Sentry, Fortinet provides network security capabilities while Network Sentry provides detailed contextual information about the endpoints, user, applications and network connections.

Networks Sentry also enables organizations to take microsegmentation to the edge. It augments the Fortinet switch, secure WiFi, firewall and gateway technologies by controlling the access layer to create a smaller threat landscape. Network Sentry adds a consistent onboarding experience, BYOD, and guest and contractor management across all types of network devices. In addition, Network Sentry works with the Fortinet security solutions to gather and add contextual information for all alerts, automate access policies and controls, and automatically quarantine threats. While Fortinet is controlling perimeter security, Network Sentry can control what files, equipment and network resources each employee or guest can access. For example, if an employee unplugs a printer and plugs in a Windows machine instead, Network Sentry will record this change and will isolate the replacement device. In this scenario, Network Sentry controls the security orchestration. When working with FortiSIEM, Network Sentry performs the same processes, but stays in constant communication with the SIEM engine, which serves as the controller. So, Network Sentry provides the visibility and contextual information to FortiSIEM, and communicates back and forth to enhance the fidelity of alerts and quarantine suspicious devices.

PARTNERSHIP

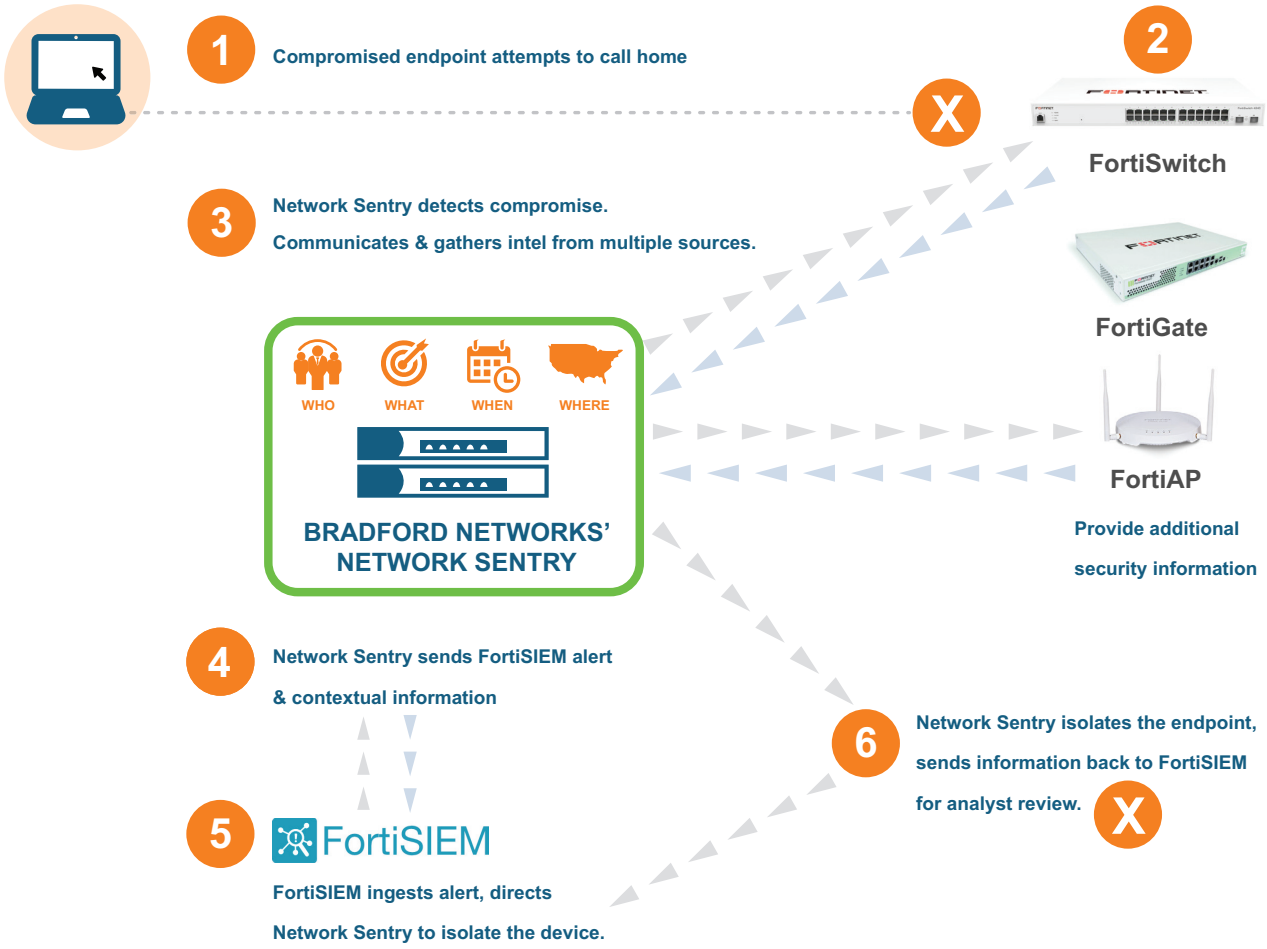
Bradford Networks is a Fortinet Fabric-Ready partner, and supports integration with FortiGate, FortiSIEM, FortiAP, FortiWLC and FortiSwitch solutions. This partnership enables both companies to share development information for even deeper integration. “Network Sentry provides complete visibility, policy-based control and automated threat response, either working with FortiSIEM as the controller, or orchestrating endpoint visibility, control and response when working with Fortinet equipment,” stated Frank Andrus, CTO of Bradford Networks. “Combining Bradford Networks and Fortinet technologies create a comprehensive security solution. These technologies both validate and complement each together to increase the fidelity of alerts and offer actionable results.”

HIGHLIGHTS

- Pre-connection scan, without requiring an agent
- Assess risk of every endpoint on the network, gather additional alert information from Fortinet hardware and, if applicable, deliver it with contextual information to FortiSIEM
- Identify vulnerable devices pre-connect or post-connect
- Reduce containment time from days to seconds
- Automatically isolate, restrict, or block compromised endpoints from the network in real-time to prevent lateral movement, or if working with FortiSIEM, deliver alerts and contextual information to FortiSIEM, and quarantine devices at its direction
- Leverage historical network forensics to trace the point of compromise
- Dynamically control every user and device’s level of access

HOW IT WORKS

The combination of Fortinet and Network Sentry provides superior layers of protection. For example, if a customer is using FortiSIEM, Network Sentry provides complete visibility and policy based control for network, mobile and IoT devices, while FortiSIEM provides the security intelligence. Bradford Networks offers complete visibility into all of these devices, gathers the alerts, and provides the contextual information — the who, what, where and when for the events. This increases the fidelity of the alerts and enables accurate triage. Network Sentry sends the event to FortiSIEM to ingest the alert, then FortiSIEM directs Network Sentry to restrict or quarantine the device if necessary. FortiSIEM and Network Sentry communicate back and forth to compile all relevant information and deliver it to a security analyst.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

February 8, 2018 8:51 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:SB-Fortinet-Brandford-Netowrks:sb-brandford-networks-fortinet